UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

MICHAEL FADULLON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CAPITAL ONE FINANCIAL CORPORATION; AMAZON WEB SERVICES, INC.; PAIGE A. THOMPSON; and DOES 1-10,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiff Michael Fadullon ("Mr. Fadullon," or "Plaintiff"), individually and on behalf of the proposed Classes defined below, alleges on personal knowledge as to himself and his own experiences and, as to all other matters, upon information and belief including investigation conducted by his attorneys.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

NATURE OF THE CASE

1. Plaintiff brings this class action lawsuit against Capital One Financial Corporation ("Capital One"), Amazon Web Services, Inc. ("AWS"), and Paige A. Thompson (collectively, "Defendants") because of their failure to protect (in the case of Capital One and AWS), or the theft of (in the case of Ms. Thompson), the confidential information of Plaintiff and many millions of other consumers—including their names, bank account numbers, Social Security numbers, addresses, phone numbers, email addresses, dates of birth, income information, banking information, credit scores, credit limits, contact information, and other private, personal information (collectively, "Personal Information"). This theft is referred to as the "Data Breach" herein.

2. Defendant Capital One is one of the largest banks in the United States, with revenues in excess of $28 billion in 2018.[1]

3. In order to apply for Capital One's banking services, an individual must provide his or her Personal Information.

4. Capital One evidently stores this information indefinitely, on the "cloud," using AWS's cloud computing services.

5. Defendant Ms. Thompson was able to exploit glaring vulnerabilities in AWS's systems to perpetrate the Data Breach at issue.

PARTIES

6. Plaintiff Michael Fadullon is a resident and citizen of the State of California, who applied for a Capital One Venture Card on February 2016, and was approved.

7. Defendant Capital One is a Delaware Corporation with its headquarters and principal place of business located in McLean, Virginia.

8. Defendant AWS is a Delaware Corporation with its headquarters in Seattle, Washington.

9. Defendant Paige A. Thompson is an individual currently incarcerated in the Seattle, Washington, area.

10. Plaintiff is unaware of the true names and capacities of the defendants sued as DOES 1-

[1] Capital One, 2018 Annual Report at 2.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

10, and therefore sues these defendants by fictitious names. Plaintiff will seek leave to amend this Complaint when and if the true identities of these DOE defendants are discovered. Plaintiff is informed and believes and thereon alleges that each of the defendants designated as a DOE is responsible in some manner for the acts and occurrences alleged herein, whether such acts or occurrences were committed intentionally, negligently, recklessly or otherwise, and that each said DOE defendant thereby proximately caused injuries and damages to Plaintiff as herein alleged, and is thus liable for the damages suffered by Plaintiff.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Classes is a citizen of a state different from Defendants, and (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

12. This Court has personal jurisdiction over Defendant Capital One because it regularly does conduct business in this District, and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

13. This Court has personal jurisdiction over Defendant AWS because it has headquarters in this District, and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

14. This Court has personal jurisdiction over Defendant Thompson because she resides and is incarcerated in this District and, on information and belief, committed the alleged hacking described herein in this District.

15. Venue is proper under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated from this District.

FACTUAL BACKGROUND

16. Capital One expressly promises it is "committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

practices."[2]

17. AWS similarly promises:

> At AWS, security is our highest priority. We design our systems with your security and privacy in mind.
>
> - We maintain a wide variety of compliance programs that validate our security controls. . . .
> - We protect the security of your information during transmission to or from AWS websites, applications, products, or services by using encryption protocols and software.
> - We follow the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card data.
> - We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal information. Our security procedures mean that we may request proof of identity before we disclose personal information to you.[3]

18. On July 29, 2019, it was revealed that AWS's and Capital One's failure to protect Capital One's customers' Personal Information resulted in the exposure of over 100 million individuals' Personal Information. According to Capital One, "[t]he largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019."[4]

19. In its press release concerning the incident, dated July 29, 2019, Capital One stated: "On July 19, 2019, we determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for credit card products and Capital One credit card customers. This occurred on March 22 and 23, 2019."[5]

20. Capital One admits that "[d]ue to the particular circumstances of this incident, the

---

[2] Capital One Online & Mobile Privacy Statement, https://www.capitalone.com/identity-protection/privacy/statement (last visited July 30, 2019).

[3] AWS Privacy Notice, Last Updated: December 10, 2018, https://aws.amazon.com/privacy/ (last visited July 30, 2019).

[4] Capital One News Release, July 29, 2019, phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-newsArticle_Print&ID=2405042 (last visited July 30, 2019).

[5] *Id.*

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

unauthorized access also enabled the decrypting of data."[6]

21. Capital One admits that a wide variety of information was compromised:

> This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond the credit card application data, [an alleged hacker] also obtained portions of credit card customer data, including:
>
> - Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information
> - Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018
>
> No bank account numbers or Social Security numbers were compromised, other than:
>
> - About 140,000 Social Security numbers of our credit card customers
> - About 80,000 linked bank account numbers of our secured credit card customers[7]

22. Federal authorities arrested an alleged hacker, Defendant Paige A. Thompson, who has been charged with perpetrating the Data Breach. *See USA v. Thompson*, Case No. 2:19-mj-00344-MAT (W.D. Wash., July 29, 2019).

23. Defendant Thompson allegedly stole the Personal Information at issue in this District, and accordingly is being charged here. *See id.*, Dkt. 1 (Complaint) at Count 1.

24. According to the Complaint against Defendant Thompson, she stated her intention to disseminate the Personal Information she stole to others, at least as of June 18, 2019, though she was not arrested until July 26-29, 2019.

25. Accordingly, Defendant Thompson had plenty of time to realize her intention of distributing the Personal Information at issue before her arrest.

26. According to the Complaint against Defendant Thompson, she was able to perpetrate the Data Breach because Capital One stored the Personal Information at issue on the "cloud," and Defendant Thompson was able to exploit vulnerabilities in the cloud services that Defendant utilized, provided by what the Complaint identifies as the "Cloud Computing Company." *Id.*

---

[6] *Id.*

[7] *Id.*

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

27. The Complaint against Defendant Thompson explains that she "formerly worked at the Cloud Computing Company," in Seattle, and additional evidence clearly suggests that this Cloud Computing Company is AWS. *Id.*[8]

28. Fundamentally, Defendants Capital One and AWS failed to provide the level of data protection that they expressly promised, thus exposing millions of individuals' Personal Information to an increased risk of misuse by unauthorized third parties (*e.g.*, identity theft).

29. Had Defendant Capital One informed its customers that it would use inadequate security measures, consumers (like Plaintiff and the members of the Classes) would not have applied for credit cards with Capital One.

30. Capital One's and AWS's failure to implement adequate security protocols jeopardized millions of consumers' Personal Information, fell well short of its promises, and diminished the value of the services provided.

31. Accordingly, Plaintiff brings suit on behalf of himself and all others similarly situated, to seek redress for Defendants' unlawful conduct.

I. Capital One is Subject to the Gramm-Leach-Bliley Act.

32. Capital One is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6809(3)(A), and thus is subject to the GLB Act.

33. The GLB Act defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

34. Capital One collects nonpublic personal information, as defined by 16 C.F.R. § 313.3(n). Accordingly, during the relevant time period Capital One was subject to the requirements of the GLB

[8] *See also, e.g.*, Brian Krebs, *Capital One Data Theft Impacts 106M People*, https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/ (last visited July 30, 2019). Mr. Krebs, a respected blogger on cybersecurity issues, includes links to what appears to be Defendant Thompson's resume, which states that she worked for "Amazon Inc. - Simple Storage Services" from May 2015 - Sep 2016, in Seattle, Washington. *See* Paige Thompson Resume Repository, https://gitlab.com/netcrave/Resume/blob/master/cv/experience.tex (last visited July 30, 2019).

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Privacy Rule, 16 C.F.R. § 313.1 *et seq.*, and is subject to numerous rules and regulations.

35. The GLB Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule, and accordingly promulgated the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), which became effective on October 28, 2014.

36. Accordingly, Capital One's conduct is governed by the Privacy Rule prior to October 28, 2014, and by Regulation P after that date.

37. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the security and confidentiality policies of the financial institution. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Capital One violated the Privacy Rule and Regulation P.

38. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Capital One violated the Safeguard Rule.

39. Capital One failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

40. Capital One's conduct (and lack thereof), resulted in a variety of failures to follow GLB mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Capital One failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the Personal Information it maintained in its data systems, instead outsourcing such responsibilities to AWS.

41. More specifically, Capital One's security failures demonstrate that it failed to honor its express and implied promises by failing to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber attacks;

b. Adequately protect Plaintiff's and the Classes' Personal Information;

c. Implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;

e. Protect against any reasonably anticipated threats or hazards to the security or integrity of Personal Information; and

f. Effectively train all members of its workforce on the policies and procedures with respect to Personal Information as necessary and appropriate for the members of its workforce

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

to carry out their functions and to maintain security of Personal Information.

42. Had Capital One implemented the above-described data security protocols, the consequences of the data exposure could have been avoided, or at least significantly reduced (as the exposure could have been detected earlier, the amount of Personal Information compromised could have been greatly reduced, and affected consumers could have been notified—and taken protective/mitigating actions—much sooner).

II. It Is Well Established that Data Breaches Lead to Identity Theft.

43. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

44. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[10]

45. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[11] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12]

---

[9] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007) ("GAO Report"), United States Government Accountability Office, http://www.gao.gov/new.items/d07737.pdf (last visited July 30, 2019).

[10] *Id.*

[11] *See Identity Theft*, Federal Trade Commission, http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited July 30, 2019).

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

46. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit various types of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[13]

47. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personal Information directly on various Internet websites making the information publicly available.

48. There may be a time lag between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"):

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

CLASS ALLEGATIONS

A. Class Definitions

49. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated.

50. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of the following Class:

All persons residing in the United States whose Personal Information was exposed in the

---

[13] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited July 30, 2019).
[14] GAO Report, at 33.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Data Breach announced by Capital One on July 29, 2019 (the "Nationwide Class").

51. Plaintiff further seeks certification of the following California Subclass:

> All persons residing in the State of California whose Personal Information was exposed in the Data Breach announced by Capital One on July 29, 2019 (the "California Subclass" and, together with the Nationwide Class, the "Classes").

52. Excluded from the Classes are: (1) Defendants, any entity or division in which any Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded, divided into further subclasses, or modified in any other way.

B. Certification of the Proposed Class is Appropriate.

53. Each of the proposed Classes meets the certification under Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3).

54. **Numerosity**: The exact number of members of the Classes is unknown to Plaintiff at this time, but on information and belief, there are over 100 million individuals in the Class, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Capital One's and AWS's records.

55. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

a. Whether Defendants Capital One and AWS failed to adequately safeguard Plaintiff's and the Classes' Personal Information;

b. Whether Defendants Capital One and AWS failed to protect or otherwise keep Plaintiff's and the Classes' Personal Information secure, as promised;

c. Whether Defendants Capital One and AWS's failure to secure Plaintiff's and the Classes' Personal Information in the manner alleged violated federal, state and local laws, or industry standards;

d. Whether Defendant Capital One's storage of Plaintiff's and the Classes' Personal

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Information in the manner alleged violated the GLB;

e. Whether Defendant Thompson distributed Plaintiff's and the Classes' Personal Information to others;

f. Whether Defendants Capital One and AWS engaged in unfair or deceptive practices by failing to properly safeguard Plaintiff's and the Classes' Personal Information as promised;

g. Whether Defendant Capital One and/or AWS failed to notify Plaintiff and members of the Classes about the Data Breach as soon as practical and without delay after the breach was discovered;

h. Whether Defendants Capital One and/or AWS acted negligently in failing to properly safeguard Plaintiff's and the Classes' Personal Information;

i. Whether Defendant Capital One's conduct described herein constitutes a breach of its implied or express contracts with Plaintiff and the members of the Class;

j. Whether Defendant Capital One should retain the money paid by Plaintiff and members of the Classes to protect their Personal Information;

k. Whether Defendant AWS should retain the money paid to it by Capital One to protect the Personal Information at issue; and

l. Whether Plaintiff and the members of the Classes are entitled to damages as a result of Defendants' conduct.

56. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

57. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Classes, and has retained counsel competent and experiences in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and Defendants have no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Classes.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

58. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the proposed Classes.

59. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Classes, and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendants' practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiff's challenge of those practices hinges on Defendants' conduct with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiff.

60. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendants. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I
Negligence
(On behalf of Plaintiff and the Classes Against Defendants Capital One and AWS)

61. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

62. Capital One required Plaintiff and members of the Classes to submit non-public Personal Information in order to apply for its credit cards and banking services.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

63. Capital One utilized AWS's cloud computing services to store, access, use, and secure the Personal Information at issue.

64. By collecting, using, storing, and profiting from this data, Defendants Capital One and AWS each had a duty of care to use reasonable means to secure and safeguard this Personal Information, to prevent disclosure of the information, and to guard the information from theft.

65. Capital One's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice in the case of a data breach.

66. As they admit in their respective privacy policies, Defendants Capital One and AWS each owed a duty to Plaintiff and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them—adequately protected Capital One's customers' Personal Information.

67. Capital One further owed a duty to use reasonable security measures as a result of the special relationship that existed between it and Plaintiff and other members of the Classes. The special relationship arose because Plaintiff and the members of the Classes entrusted Capital One with their confidential Personal information in order to acquire and use Capital One's banking services. Only Capital One was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Classes from such a data breach.

68. Capital One's duty to use reasonable security measures also arose under GLB, under which Capital One was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

69. In addition, Defendants Capital One and AWS had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

70. Defendants Capital One and AWS breached their common law, statutory, and other

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

duties by failing to use reasonable measures to protect consumers' Personal Information and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and members of the Classes' Personal Information;

b. failing to adequately monitor the security of Capital One's customer data on AWS's networks;

c. allowing unauthorized access to Plaintiff's and other members of the Classes' Personal information;

d. failing to recognize in a timely manner that Plaintiff's and other members of the Classes' Personal information had been compromised; and

e. failing to warn Plaintiff and other members of the Classes in a timely manner that their Personal Information had been compromised.

71. It was foreseeable that failure to use reasonable measures to protect this Personal Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other members of the Classes. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and other members of the Classes were reasonably foreseeable.

72. It was and remains foreseeable that the failure to adequately safeguard Personal Information will result in one or more of the following injuries to Plaintiff and other members of the Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

73. Accordingly, Plaintiff, on behalf of himself and other members of the Classes, seeks an order declaring that Defendants' conduct constitutes negligence, and awarding them damages in an amount to be determined at trial.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

COUNT II
Violation of the Washington Consumer Protection Act
(On behalf of Plaintiff and the Nationwide Class Against Defendants Capital One and AWS)

74. Plaintiff incorporates the allegations above as if fully set forth here.

75. Washington's Consumer Protection Act, RCW §§ 19.86.010, *et seq.* ("CPA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

76. To achieve that goal, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce. . . ." RCW § 19.86.020. An unfair or deceptive business practice is one that is likely to deceive a substantial portion of the public or otherwise affect public interest.

77. Defendants Capital One and AWS expressly represented that they would take reasonable measures to protect the Personal Information compromised in the Data Breach.

78. Consistent with their privacy policy representations, Defendants Capital One and AWS accepted responsibility for securing Plaintiff's and other Class members' Personal Information. Given that it was Defendants' responsibility for creating, overseeing, maintaining, and otherwise implementing their own data security practices, Defendants knew (or should have known) that they were not adequately protecting the compromised Personal Information in accordance with their express guarantees.

79. Defendants' failure to notify Plaintiff and other Class members promptly about the Data Breach was both unfair and misleading, because this failure ran contrary to Defendants' promised confidentiality practices, and exposed Plaintiff and other Class members to additional (and unnecessary) harm, and otherwise offended public policy.

80. Consumers—like Plaintiff and other Class members—value their privacy. Companies that offer adequate data security protections are more valuable to consumers than those with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with adequate security practices over one with substandard security practices.

81. Because of this consumer preference for data security, a bank safeguarding and protecting Personal Information in accordance with the GLB, other federal, state and local laws, and

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

industry standards—in addition with its own affirmative representations of its data security practices—commands a higher customer based for its services than a bank with substandard security.

82. Similarly, a cloud computing company's services are worth more if it provides adequate security, as AWS represents it will provide.

83. Prior to the Data Breach, neither Plaintiff nor the general public knew that neither Defendant Capital One nor AWS was implementing the data security and privacy protocols they promised in their own consumer-facing representations. These Defendants knew that customers would not give these Defendants their business if customers knew Defendants could not or would not protect such Personal Information, as they represented they would. And rather than implement the data security and privacy protocols they promised, Defendants actively concealed their true practices and protocols (which were of material concern to all of their customers), while at the same time expressly promising that Personal Information would be protected as described above.

84. Had Plaintiff and other Class members known that Defendant Capital One did *not* actually implement its promised data security and privacy protocols, they would not have been willing to provide Defendant with their Personal Information.

85. Defendants' unfair acts or practices occurred in their trade or business and have proximately caused injury to Plaintiff and to other Class members. Defendants' general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of their misconduct may last for years (*e.g.*, affected individuals could experience identity theft for years). As a direct and proximate result of Defendants' unfair acts, Plaintiff and other Class members have suffered actual injuries, including without limitation investing substantial time or money in monitoring and remediating the harm inflicted upon them by the Data Breach.

86. As a result of Defendants' conduct, Plaintiff and other Class members have suffered actual damages, including the lost value of their privacy, the lost value of their Personal Information, and lost property in the form of their breached and compromised Personal Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse,

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

87. Accordingly, Plaintiff, on behalf of himself and members of the proposed Class, seeks to enjoin further violation and recover actual damages and treble damages (where applicable), together with the costs of bringing this suit, including reasonable attorneys' fees.

88. With respect to injunctive relief, Plaintiff, on behalf of himself and members of the proposed Class, seeks an Order requiring Defendants to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering Defendants to correct any problems or issues detected by such third-party security auditors promptly; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train their security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Capital One's AWS-maintained cloud network is compromised, hackers cannot gain access to other portions of either Defendants' systems; (5) purge, delete, and destroy in a reasonably secure manner Personal Information not necessary for Capital One's provisions of services to such consumers; (6) conduct regular database scanning and securing checks; (7) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) meaningfully educate all Class members about the threats they face as a result of the loss of their confidential financial, personal, information to third parties, as well as the steps affected individuals should take to protect themselves.

COUNT III
Violation of Washington Data Breach Disclosure Law
(On behalf of Plaintiff and the Nationwide Class Against Capital One and AWS)

89. Plaintiff incorporates the foregoing allegations as if fully set forth here.

90. RCW § 19.255.010(2) provides that "[a]ny person or business that maintains

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *See* RCW § 19.255.010(2) (2005).

91. The Data Breach described above resulted in an "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendants and, therefore, experienced a "breach of the security of [their] system[s]," as defined by RCW § 19.255.010(4) (2005).

92. Defendants failed to disclose the breach of Capital One's data on AWS's systems immediately after discovering the Data Breach. Defendants unreasonably delayed informing Plaintiff and other Class members about the Data Breach after they knew or should have known that the Data Breach had occurred.

93. Defendants' failure to provide notice immediately after discovering the Data Breach is a violation of RCW § 19.255.010.

COUNT IV
Violation of California Data Breach Law
(On behalf of Plaintiff and the California Subclass Against Capital One and AWS)

94. Plaintiff incorporates the foregoing allegations as if fully set forth here.

95. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

96. The Private Information taken in the Data Breach fits within the definition of "Personal Information" in Cal. Civil Code § 1798.80.

97. Plaintiff and California Subclass members provided their Personal Information to Defendant Capital in order to use its banking services, and thus qualify as "Customer[s]" as defined in Cal. Civil Code § 1798.80.

98. Defendants failed to dispose of Plaintiff's and others' Personal Information when it was

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

no longer needed, violating Cal. Civil Code § 1798.81.

99. By failing to implement reasonable measures to protect the Personal Information in their possession, Defendants violated Cal. Civil Code § 1798.81.5.

100. In addition, by failing to promptly notify all who were affected by the Data Breach that their Personal Information had been acquired by hackers, Defendants violated Cal. Civil Code § 1798.82.

101. As a direct or proximate result of Defendants' violations of Cal. Civil Code §§ 1798.81, 1798.81.5, and 1798.82, Plaintiff and California Subclass members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

102. Defendants' violations of Cal. Civil Code §§ 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless.

103. In addition, by violating Cal. Civil Code §§ 1798.81, 1798.81.5, and 1798.82, Defendants may be enjoined under Cal. Civil Code § 1798.84(e).

104. Defendants' violations of Cal. Civil Code §§ 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

105. Plaintiff accordingly requests that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering Defendants to correct any problems or issues detected by such third-party security auditors promptly; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train their security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Capital One's AWS-maintained cloud network is compromised, hackers cannot gain access to other portions of either of Defendants' systems; (5) purge, delete, and destroy in a reasonably secure manner Personal Information not necessary for Capital One's provisions of services to such consumers; (6)

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

conduct regular database scanning and securing checks; (7) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) meaningfully educate all California Subclass members about the threats they face as a result of the loss of their confidential financial, personal, information to third parties, as well as the steps affected individuals should take to protect themselves.

106. Plaintiff further requests that the Court require Defendants to identify and notify all members of the California Subclass who have not yet been informed of the Data Breach, and to notify affected consumers of any future data breaches by email within 24 hours of Defendants' discovery of a breach or possible breach and by mail within 72 hours.

107. Plaintiff and the California Subclass are entitled to actual damages in an amount to be determined at trial under Cal. Civil Code Section 1798.84.

108. Plaintiff and the California Subclass also are entitled to an aware of attorney fees and costs under Cal. Civil Code Section 1798.84.

COUNT V
Conversion
(On behalf of Plaintiff and the Nationwide Class Against Defendant Thompson)

109. Plaintiff incorporates the foregoing allegations as if fully set forth here.

110. By hacking into Defendants Capital One's and AWS's computerized systems to take Plaintiff's Personal Information, Defendant Thompson eviscerated the confidentiality of that Personal Information.

111. Plaintiff and other Class members did not consent to Defendant Thompson's actions.

112. As a result of Defendant Thompson's conduct, Plaintiff and other Class members have suffered actual damages, including the lost value of their privacy, the lost value of their Personal Information, and lost property in the form of their breached and compromised Personal Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

113. Plaintiff seeks damages on behalf of himself and other Class members from Defendant Thompson compensating them for their injuries.

114. Plaintiff further seeks an injunction preventing Defendant Thompson from working in any capacity in which she again could gain access to knowledge concerning cloud computing industry vulnerabilities.

COUNT VI
Breach of Express Contract
(On behalf of Plaintiff and the National Data Breach Class Against Defendant Capital One)

115. Plaintiff incorporates the foregoing allegations as if fully set forth here.

116. Plaintiff and members of the Classes entered into valid and enforceable contracts with Defendant Capital One under which it promised to provide data protection services to them, along with banking services. Plaintiff and members of the Classes agreed to, among other things, pay money for such services, and use Defendant's credit cards as opposed to credit cards from other issuers, thereby generating revenues for Defendant in the form of processing fees charged to merchants and interest charged to consumers.

117. Both aspects of Plaintiff's and the other Class members' agreements with Defendant (*i.e.*, the provision of banking and data protection services) were material.

118. Defendant expressly promised Plaintiff and other Class members to safeguard and protect the confidentiality of their Personal Information in accordance with GLB regulations; federal, state and/or local laws; and industry standards.

119. Defendant promised to comply with all GLB regulations, federal, state and/or local laws, and industry standards to make sure that Plaintiff's and the members of the Classes' Personal Information was protected.

120. These contracts required that Defendant protect Plaintiff's and other Class members' Personal Information and to prevent unauthorized access to such information.

121. Unfortunately, Defendant Capital One did not safeguard this Personal Information. Specifically, Defendant did not comply with its promises to abide by GLB, federal, state and/or local

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

laws, or industry standards.

122. The failure to meet these promises and obligations constitutes a breach of express contract.

123. Because Defendant allowed unauthorized access to Plaintiff's and other Class members' Personal Information, and otherwise failed to safeguard the Personal Information, as promised, Defendant breached its contracts with Plaintiff and other Class members.

124. A meeting of the minds occurred, as Plaintiff and other Class members agreed to, among other things, provide Defendant with their accurate and complete information (including their Personal Information) and to use Defendant's payment cards in exchange for its agreement to, among other things, protect their Personal Information.

125. Defendant breached these contracts by failing to implement (or adequately implement) sufficient security measures to protect Plaintiff's and other Class members' Personal Information.

126. As a result of Defendant's conduct, Plaintiff and members of the Classes have suffered actual damages.

127. Accordingly, Plaintiff, on behalf of themselves and the other members of the Classes seek an order declaring that Defendant's conduct constitutes breach of express contract, and awarding them damages in an amount to be determined at trial.

REQUEST FOR RELIEF

Plaintiff, on behalf of themselves and the Classes, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of Plaintiff and the Classes defined above, appointing Plaintiff as representatives of their respective Classes, and appointing their counsel as Class Counsel;

B. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Defendants Capital One and AWS to protect all data collected through the course of their business in accordance with GLB regulations, industry standards, and federal, state and/or local laws; (iii) requiring Defendants Capital One and AWS to engage third-party security

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants Capital One and AWS to promptly correct any problems or issues detected by such third-party security auditors; (iv) requiring Defendants Capital One and AWS to engage third-party security auditors and internal personnel to run automated security monitoring; (v) requiring Defendants Capital One and AWS to audit, test, and train their security personnel regarding any new or modified procedures; (vi) requiring Defendants Capital One and AWS to segment data by, among other things, creating firewalls and access controls so that if one area of either Defendant's network is compromised, hackers cannot gain access to other portions of Defendants' systems; (vii) requiring Defendants Capital One and AWS to purge, delete, and destroy in a reasonably secure manner Personal Information not necessary for Capital One's provisions of services; (viii) requiring Defendants Capital One and AWS to conduct regular database scanning and securing checks; (ix) requiring Defendants Capital One and AWS to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (x) requiring Defendants Capital One and AWS to meaningfully educate all class members about the threats they face as a result of the loss of their confidential Personal Information to third parties, as well as the steps affected individuals must take to protect themselves.

A. Awarding damages to Plaintiff and the Classes in an amount to be determined at trial;

B. Awarding restitution to Plaintiff and the Classes in an amount to be determined at trial;

C. Awarding Plaintiff and the Classes their reasonable litigation expenses and attorneys' fees;

D. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable; and

E. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff requests a trial by jury.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Respectfully submitted,

Dated: July 30, 2019

KELLER ROHRBACK L.L.P.

By: */s/ Cari C. Laufenberg*

Cari Campen Laufenberg (WSBA 34354)
Lynn Lincoln Sarko (WSBA 16569)
T. David Copley (WSBA 19379)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel: (206) 623-1900
Fax: (206) 623-3384
claufenberg@kellerrohrback.com
lsarko@kellerrohrback.com
dcopley@kellerrohrback.com

Christopher Springer, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Tel: (805) 456-1496
Fax: (805) 456-1497
cspringer@kellerrohrback.com

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson

Tina Wolfson, *pro hac vice forthcoming*
Theodore Maya, *pro hac vice forthcoming*
Bradley K. King, *pro hac vice forthcoming*
Ruhandy Glezakos, *pro hac vice forthcoming*
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
tmaya@ahdootwolfson.com
bking@ahdootwolfson.com
rglezakos@ahdootwolfson.com